Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application:

Listing of Claims:

1-2. (canceled)

3. (currently amended) The method of ~~claim 1~~ claim 24, wherein the producing of the certificate occurs at an initial power-on of the platform.

4. (currently amended) The method of ~~claim 2~~ claim 24, wherein the ~~producing of the certificate~~ operation of generating an attestation key pair comprises:

loading, into the platform, boot code provided by an agent of an outside entity;

booting the platform from the boot code ~~stored in a platform readable medium loaded by an~~ provided by the agent; and

after booting the platform from the boot code provided by the agent, executing an applet ~~running within the isolated area of the system memory~~ in isolated execution mode to generate the attestation key pair.

5. (currently amended) The method of claim 4, wherein the producing of the certificate further comprises ~~encrypting the public attestation key~~ signing the certificate with a private key ~~held by the agent~~ of the outside entity.

6. (currently amended) The method of ~~claim 1~~ claim 24, wherein the producing of the certificate comprises:

~~encrypting the public attestation key using~~ signing the certificate with a private key held by ~~an original equipment~~ a manufacturer of the platform.

7. (currently amended) The method of ~~claim 1~~ claim 24 further comprising:

receiving a challenge message from a remotely located platform, the challenge message including a nonce.

8. (original) The method of claim 7 further comprising:

generating a response message for transmission to the remotely located platform, the response message including the certificate, the nonce and a hash value of an audit log.

9. (original) The method of claim 8, wherein the nonce and the hash value are signed with the private attestation key.

10. (currently amended) A platform comprising:

a processor to operate selectively in ~~one of~~ distinct modes including a normal execution mode and an isolated execution mode;

~~an input/output control hub in communication with the processor, the input/output control hub to generate an attestation key pair and to store an audit log being a listing of data representing a plurality of software modules loaded within the platform~~

storage in communication with the processor, the storage comprising a system memory to include an isolated area that is accessible only when the processor is operating in isolated execution mode;

key generation instructions encoded in the storage, the key generation instructions to generate an attestation key pair for the platform while executing in isolated execution mode, wherein the attestation key pair comprises a private attestation key and a public attestation key; and

a certificate in the storage, wherein the certificate attests that the platform uses isolated execution mode to protect the private key.

11. (currently amended) The platform of claim 10, wherein the ~~plurality of software modules include~~ storage comprises a processor nub to execute in isolated execution mode and an operating system nub to execute in isolated execution mode.

12. (original) The platform of claim 10 further comprising at least one input/output device allowing communications with a remotely located platform.

13. (currently amended) The platform of claim 10 further ~~comprising~~ comprising:

a device in communication with the processor; and

a token link coupled to the ~~input/output control hub~~ device, the token link providing a communication path for a token.

14. (currently amended) The platform of claim 13 wherein the token stores [[a]] the private attestation key of the attestation key pair.

15. (canceled)

16. (currently amended) The platform of ~~claim 15~~ claim 13, wherein the device comprises a ~~the~~ protected memory ~~includes a plurality of single-write, multiple-read control registers~~ to hold an audit log of software modules loaded on the platform in isolated execution mode.

17. (currently amended) The platform of ~~claim 15~~ claim 13, wherein the device is an input/output control ~~nub~~ hub.

18. (canceled)

19. (currently amended) A method comprising:

generating an attestation key pair for a platform;

storing a private attestation key of the attestation key pair into isolated memory of the platform, the isolated memory being accessible to a processor of the platform only when the processor operates in isolated execution mode, wherein the isolated memory comprises hardware-protected memory; and

producing a certificate including the public attestation ~~key~~ key, the certificate to attest that the platform stores the private attestation key ~~is stored~~ in the ~~hardware protected~~ isolated memory.

20. (original) The method of claim 19, wherein the hardware-protected memory includes single-write, multiple-read control registers.

21. (canceled)

22. (original) The method of claim 19, wherein the producing of the certificate occurs at an initial power-on of the platform.

23. (currently amended) The method of claim 19, wherein the ~~producing of the certificate~~ operation of generating an attestation key pair comprises:

booting [[a]] the platform ~~including the hardware-protected memory~~ from code ~~stored in a readable medium loaded~~ provided by an agent of an outside entity; and

~~executing an applet stored in the hardware-protected memory~~ using the code provided by the agent to generate the attestation key pair.

24. (new) A method comprising:

generating an attestation key pair in a platform that supports isolated execution mode, wherein the platform comprises a processor capable of operating in isolated execution mode and a system memory to include an isolated area that is accessible only when the processor is operating in isolated execution mode, and wherein the attestation key pair includes a private attestation key and a public attestation key; and

producing a certificate for the platform to attest that the platform uses isolated execution mode to protect the private key.